ATTACHMENT A-1

PERSON TO BE SEARCHED:

Stephen J. RIVITZ, DOB: October, 7, 1948, Social Security Number: 014-40-0732, of 161 Cady Ave. Warwick, RI. RIVITZ, pictured below, is described as a white male, 71 years old, 5'7, weighing 178 pounds with balding/grey hair ("SUBJECT PERSON").

ATTACHMENT B-1

A. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349), Money Laundering (U.S.C. § 1956(h)), Conspiracy to Commit Theft of Public Money (18 U.S.C. § 371), and Theft of Public Money (18 U.S.C. § 641) ("Specified Federal Offenses"):

1. Records and other materials relating to the receipt of funds from the Department of Treasury and/or any state unemployment system, to include the Washington state unemployment system.

2. Records and other materials relating to fraudulent tax returns and fraudulent tax refunds, including personal identification (PII) used in furtherance of such returns and the receipt of tax refunds in the names of persons other than Stephen RIVITZ.

3. Records and other materials relating to the closure of bank accounts.

4. Records and other materials relating to notice from banks, RI Department of Elderly Affairs, or other third parties relating to Stephen RIVITZ involvement in suspected fraud and receipt of suspected fraudulent funds.

5. Records and other materials including notes, addresses, ledgers, envelopes, and packaging materials, relating to receipt and transfer / disposition of cash, money orders, checks, or wire transfers that were sent or received to/from known and unknown conspirators.

6. Records relating to any communications and meetings by, between, and among "Mary Rose", "Mike," "Gary" and known and unknown conspirators relating to the receipt, solicitation, and transfer of funds.

7. Records relating to the transfer of funds to Nigeria.

8. Records relating to the use, possession, and control of cellular telephones seized from the SUBJECT PREMISES and/or SUBJECT VEHICLE.

9. Records relating to any communications with co-conspirators, including telephone, electronic, or in person communications with co-conspirators in relation to the Specified Federal Offenses, the transfer and receipt of funds between the subjects of the investigation and other persons;

10. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles including by not limited to the SUBJECT VEHICLE, precious metals, jewelry, or other items obtained with the proceeds from a fraud;

11. Any records which document an association with co-conspirators, including texts, contact lists, photographs, video and audio recordings;

12. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) relating to individuals identified as victims in this investigation;

13. Banking, money remitter, and financial institution records, including but not limited to bank statements, credit card statements, canceled checks, money orders, deposit slips, orders for receipt or sending of money transfer by wire, checking and savings books, financial institution statements, and records of safe deposit boxes;

14. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "COMPUTER")[1]:

[1] The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
h. evidence of the times the COMPUTER was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
k. records of or information about Internet Protocol addresses used by the COMPUTER; and
l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

15. Routers, modems, and network equipment used to connect computers to the Internet.

---

recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMS, and other magnetic or optical media.

16. As used in this Attachment, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

17. With respect to any and all electronically stored information in cellular telephones, in addition to the information described herein, agents may also access, record and seize the following:
    a. Telephone numbers of incoming/outgoing calls stored in the call registry;
    b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
    c. Any incoming/outgoing text messages relating to the above criminal violations;
    d. Telephone subscriber information;
    e. The telephone numbers stored in the cellular telephone and/or PDA;
    f. records relating to the use, possession, and control of any cellular telephones seized;
    g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above criminal violations.

18. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

B. SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS

1. During the execution of this search warrant, law enforcement is permitted to:

   a. depress the user's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
   b. hold the device in front of the user's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT A-2

PREMISES TO BE SEARCHED

The SUBJECT PREMISES is the premises at 161 Cady Avenue, Warwick, RI. SUBJECT PREMISES is described as a single-family residence. SUBJECT PREMISES has a brick exterior with a white front door that is accessed by going up three steps.

The area to be searched at the SUBJECT PREMISES includes the room rented by RIVITZ and common areas, to include locked containers and safes, lockers, sheds, and any visible structures and outbuildings associated with the SUBJECT PREMISES and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, digital devices, and any other storage locations within SUBJECT PREMISES in the room rented by RIVITZ.

The search shall also include any person located at the SUBJECT PREMISES, as defined above, at the time the search warrant is executed, and any computers, cellular telephones, storage media/medium, briefcases, backpacks, wallets, and purses on such persons.

ATTACHMENT B-2

A. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349), Money Laundering (U.S.C. § 1956(h)), Conspiracy to Commit Theft of Public Money (18 U.S.C. § 371), and Theft of Public Money (18 U.S.C. § 641) ("Specified Federal Offenses"):

1. Records and other materials relating to the receipt of funds from the Department of Treasury and/or any state unemployment system, to include the Washington state unemployment system.

2. Records and other materials relating to fraudulent tax returns and fraudulent tax refunds, including personal identification (PII) used in furtherance of such returns and the receipt of tax refunds in the names of persons other than Stephen RIVITZ.

3. Records and other materials relating to the closure of bank accounts.

4. Records and other materials relating to notice from banks, RI Department of Elderly Affairs, or other third parties relating to Stephen RIVITZ involvement in suspected fraud and receipt of suspected fraudulent funds.

5. Records and other materials including notes, addresses, ledgers, envelopes, and packaging materials, relating to receipt and transfer / disposition of cash, money orders, checks, or wire transfers that were sent or received to/from known and unknown conspirators.

6. Records relating to any communications and meetings by, between, and among "Mary Rose", "Mike," "Gary" and known and unknown conspirators relating to the receipt, solicitation, and transfer of funds.

7. Records relating to the transfer of funds to Nigeria.

8. Records relating to the use, possession, and control of cellular telephones seized from the SUBJECT PREMISES and/or SUBJECT VEHICLE.

9. Records relating to any communications with co-conspirators, including telephone, electronic, or in person communications with co-conspirators in relation to the Specified Federal Offenses, the transfer and receipt of funds between the subjects of the investigation and other persons;

10. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles including by not limited to the SUBJECT VEHICLE, precious metals, jewelry, or other items obtained with the proceeds from a fraud;

11. Any records which document an association with co-conspirators, including texts, contact lists, photographs, video and audio recordings;

12. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) relating to individuals identified as victims in this investigation;

13. Banking, money remitter, and financial institution records, including but not limited to bank statements, credit card statements, canceled checks, money orders, deposit slips, orders for receipt or sending of money transfer by wire, checking and savings books, financial institution statements, and records of safe deposit boxes;

14. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "COMPUTER")[2]:

[2] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
h. evidence of the times the COMPUTER was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
k. records of or information about Internet Protocol addresses used by the COMPUTER; and
l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

15. Routers, modems, and network equipment used to connect computers to the Internet.

---

recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMS, and other magnetic or optical media.

16. As used in this Attachment, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

17. With respect to any and all electronically stored information in cellular telephones, in addition to the information described herein, agents may also access, record and seize the following:
    a. Telephone numbers of incoming/outgoing calls stored in the call registry;
    b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
    c. Any incoming/outgoing text messages relating to the above criminal violations;
    d. Telephone subscriber information;
    e. The telephone numbers stored in the cellular telephone and/or PDA;
    f. records relating to the use, possession, and control of any cellular telephones seized;
    g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above criminal violations.

18. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

4. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

5. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

6. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

B. SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS

2. During the execution of this search warrant, law enforcement is permitted to:

   a. depress the user's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
   b. hold the device in front of the user's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order

ATTACHMENT A-3

VEHICLE TO BE SEARCHED

A 2008 Toyota Prius (VIN# JTDKB20U383313202), color silver, registered in the name of Stephen Rivitz, 161 Cady Ave., Warwick, Rhode Island, Rhode Island plate number 473409 (hereinafter referred to as "the SUBJECT VEHICLE").

.

The area to be searched in the SUBJECT VEHICLE includes all trash containers, debris boxes, storage lockers, locked containers and safes, lockers, within the SUBJECT VEHICLE and shall extend into safes, briefcases, backpacks, wallets, purses, digital devices, and any other storage locations within the SUBJECT VEHICLE.

The search shall also include any person located in the SUBJECT VEHICLE, as defined above, at the time the search warrant is executed, and any computers, cellular telephones, storage media/medium, briefcases, backpacks, wallets, and purses on such persons.

ATTACHMENT B-3

A. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349), Money Laundering (U.S.C. § 1956(h)), Conspiracy to Commit Theft of Public Money (18 U.S.C. § 371), and Theft of Public Money (18 U.S.C. § 641) ("Specified Federal Offenses"):

1. Records and other materials relating to the receipt of funds from the Department of Treasury and/or any state unemployment system, to include the Washington state unemployment system.

2. Records and other materials relating to fraudulent tax returns and fraudulent tax refunds, including personal identification (PII) used in furtherance of such returns and the receipt of tax refunds in the names of persons other than Stephen RIVITZ.

3. Records and other materials relating to the closure of bank accounts.

4. Records and other materials relating to notice from banks, RI Department of Elderly Affairs, or other third parties relating to Stephen RIVITZ involvement in suspected fraud and receipt of suspected fraudulent funds.

5. Records and other materials including notes, addresses, ledgers, envelopes, and packaging materials, relating to receipt and transfer / disposition of cash, money orders, checks, or wire transfers that were sent or received to/from known and unknown conspirators.

6. Records relating to any communications and meetings by, between, and among "Mary Rose", "Mike," "Gary" and known and unknown conspirators relating to the receipt, solicitation, and transfer of funds.

7. Records relating to the transfer of funds to Nigeria.

8. Records relating to the use, possession, and control of cellular telephones seized from the SUBJECT PREMISES and/or SUBJECT VEHICLE.

9. Records relating to any communications with co-conspirators, including telephone, electronic, or in person communications with co-conspirators in relation to the Specified Federal Offenses, the transfer and receipt of funds between the subjects of the investigation and other persons;

10. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles including by not limited to the SUBJECT VEHICLE, precious metals, jewelry, or other items obtained with the proceeds from a fraud;

11. Any records which document an association with co-conspirators, including texts, contact lists, photographs, video and audio recordings;

12. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) relating to individuals identified as victims in this investigation;

13. Banking, money remitter, and financial institution records, including but not limited to bank statements, credit card statements, canceled checks, money orders, deposit slips, orders for receipt or sending of money transfer by wire, checking and savings books, financial institution statements, and records of safe deposit boxes;

14. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "COMPUTER")[3]:

[3] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
h. evidence of the times the COMPUTER was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
k. records of or information about Internet Protocol addresses used by the COMPUTER; and
l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

15. Routers, modems, and network equipment used to connect computers to the Internet.

---

recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMS, and other magnetic or optical media.

16. As used in this Attachment, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

17. With respect to any and all electronically stored information in cellular telephones, in addition to the information described herein, agents may also access, record and seize the following:
    a. Telephone numbers of incoming/outgoing calls stored in the call registry;
    b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
    c. Any incoming/outgoing text messages relating to the above criminal violations;
    d. Telephone subscriber information;
    e. The telephone numbers stored in the cellular telephone and/or PDA;
    f. records relating to the use, possession, and control of any cellular telephones seized;
    g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above criminal violations.

18. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

7. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

8. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

9. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

B. SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS

3. During the execution of this search warrant, law enforcement is permitted to:

   a. depress the user's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
   b. hold the device in front of the user's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.